Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 30 novembre 2000
N° CERTA-2000-ALE-016

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Connexion Wanadoo

Gestion du document

Référence	CERTA-2000-ALE-016
Titre	Connexion à Wanadoo
Date de la première version	30 novembre 2000
Date de la dernière version	–
Source(s)	Service sécurité de Wanadoo
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- surfacturation des connexions à Internet ;
- interception des communications sur Internet ;
- tous les risques liés aux exécutables inconnus : virus et chevaux de Troie par exemple.

2 Systèmes affectés

Ordinateurs fonctionnant sous l'un des systèmes d'exploitation Windows pour assurer la connexion aux services `Wanadoo` ou `Wanadoo Plus`.

3 Résumé

Le mode de diffusion d'un outil de modification de la configuration d'accès à Internet peut faciliter la diffusion de chevaux de Troie.

4 Description

Wanadoo change le 30 novembre le numéro de téléphone de connexion à l'Internet.

Le service clientèle de Wanadoo invite ses usagers à changer leur configuration Internet afin de prendre en compte ce nouveau numéro.

Un utilitaire est proposé en téléchargement sur un site Web pour les utilisateurs qui se connectent à Internet à l'aide d'une machine fonctionnant sous l'un des systèmes d'exploitation Windows.

L'utilitaire fourni par Wanadoo n'est pas en question.

Le téléchargement de cet utilitaire (simple connexion HTTP) n'offre pas de garantie sur la qualité du fichier téléchargé. En particulier un pirate aguerri pourrait, en détournant le serveur de nom, se faire passer pour Wanadoo et proposer un autre utilitaire que celui fourni par Wanadoo. C'est la porte ouverte aux chevaux de Troie.

En particulier, il existe des chevaux de Troie qui fonctionnent sur le même principe mais qui changent les paramètres de configuration de sorte que vos accès Internet se fasse non pas au travers du numéro de téléphone de votre fournisseur d'accès mais par celui d'un fournisseur d'accès à l'étranger. Ceci a plusieurs inconvénients pour l'abonné :

1° le plus flagrant est l'augmentation considérable de la facture téléphonique pour un trafic Internet équivalent ;

2° le second est le risque d'interception chez le fournisseur d'accès pirate, qui a le loisir de faire toutes les analyses de vos communications dans un pays qui n'offre pas les mêmes protections juridiques qu'en France (loi « informatique et liberté » notamment).

A la date de rédaction de ce document le problème est du domaine du risque. Aucun incident de ce type n'a été rapporté concernant l'outil proposé en téléchargement par Wanadoo. Cependant, le danger réside dans le fait qu'un mode d'accès non sûr à un logiciel critique est proposé par une source fiable (un fournisseur d'accès reconnu). Cela pourrait conduire des administrateurs systèmes à être moins vigilants en acceptant de tels logiciels de sources non fiables (serveurs ftp publics, ...).

5 Contournement provisoire

Le service sécurité de Wanadoo propose aux utilisateurs de Windows la procédure suivante pour changer manuellement la configuration de l'accès à Internet :

1° ouvrir le « Poste de travail », puis l'« Accès Réseau à Distance » ;

2° Pour toutes les fichiers de configuration des connections « Wanadoo », « Wanadoo Plus », etc. :

- ouvrir ce fichier et vérifier si le numéro est le « 08 36 01 93 01 »
- si oui, le remplacer par « 08 60 00 84 84 »
- valider et refermer.

6 Solution

La solution consiste à insister auprès de son fournisseur d'accès (quel qu'il soit) afin d'obtenir des moyens sûrs de mettre à jour les paramètres de connexions :

- une procédure manuelle ;
- un site de téléchargement sécurisé (HTTPS par exemple).

Gestion détaillée du document

30 novembre 2000 version initiale.